

**AFFIDAVIT**

I, Selena Deacons, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

- 1) I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—a black iPhone more fully described in Attachment A—which is currently in law enforcement possession, and the extraction from that property of electronically stored information as described in Attachment B.
- 2) There is probable cause to believe that a search of the device will lead to evidence of violations of 21 U.S.C. §§ 846, 841(a), and 952, conspiracy to possess and possession with intent to distribute controlled substances, and importation of controlled substances.
- 3) The facts that establish the probable cause necessary for issuance of the Order are personally known to me, are contained in official government or business records I have reviewed, or have been told to me directly by other members of the investigative team, which includes federal, state, or local law enforcement officers with whom I have worked on this investigation. As this affidavit is submitted for a limited purpose, it does not contain all aspects of this investigation, but only sufficient information to establish probable cause in support of the issuance of an Order for the examination of the device.
- 4) I am a Special Agent with the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) and have been so employed since October of 2023. I have approximately eight months of experience conducting investigations into violations of federal law, including drug trafficking.
- 5) As a Special Agent with HSI, I am responsible for investigating violations of federal law, to include violations of Title 8, Title 18, Title 19, Title 21, and Title 31 of the United States Code. In preparing to become a Special Agent, I attended the Criminal Investigator

Training Program and the HSI Special Agent Training at the Federal Law Enforcement Training Center in Glyncro, Georgia.

6) Prior to becoming a Special Agent with HSI, I was a U. S. Customs and Border Protection Officer for Nogales, AZ. I was employed by the Department of Homeland Security as a Customs and Border Protection officer for approximately three years.

7) During my law enforcement career, I have participated in drug trafficking investigations involving violations of state and federal law. I have been involved in coordinated surveillance operations, conducted seizures, and assisted in interrogations of violators and interviews of witnesses. I am familiar with the federal procedures involved in the execution of federal search warrants. I received Title III training in the academy and received guidance in Title III investigations from co-workers with extensive experience.

8) Through my training and experience, including on-the-job discussions with other law enforcement agents and cooperating suspects, I am familiar with the operational techniques and structure of contraband smuggling organizations. My responsibilities include conducting investigations into Drug Trafficking Organizations (DTO) and individuals who derive substantial income from the illicit movement and distribution of narcotics and firearms.

9) Through training and experience I know:

a) That contraband smugglers maintain books, records, receipts, notes, ledgers, personal computers, cellular phones, money orders, and other papers relating to the movement and storage of narcotics;

b) That large-scale narcotics traffickers often utilize electronic equipment such as cellular telephones, personal digital assistants (PDAs), computers, telex machines, facsimile machines, and telephone answering machines to generate, transfer, count, record, and store information related to narcotic trafficking;

c) That narcotics smugglers commonly use cellular telephones to communicate with their associates and to facilitate movement and housing of narcotics and firearms. These cellular telephones usually contain electronically stored data on or within the cellular telephones, including, but not limited to, contact names and numbers of associates, call details including call history, electronic mail (email) messages, text messages and text message history, and digital images of the narcotics and firearms trafficking associates and activity, all of which can be used to identify and locate associates, to identify methods of operation of the traffickers, and to corroborate other evidence obtained during the course of the current investigation;

d) That narcotics traffickers take, or cause to be taken, photographs and videos of themselves, their associates, their property, and their narcotics and firearms. That these smugglers usually maintain these photographs within their possession, in their residences, vehicles, businesses, cellular telephones, or other locations which they maintain dominion and control over.

10) This affidavit is based on information which is personally known by me or which I learned from other law enforcement agents. This affidavit is intended to show only that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

#### **IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

11) The purpose of this warrant is to search one (1) Apple iPhone (Target Device 1), as further described in Attachment A.

12) Target Device 1 is currently in law enforcement custody and is being held at the HSI Nogales office; 41 Paseo De Yucatan, Rio Rico, AZ 85648.

13) The applied-for warrant would authorize the forensic examination of Target Device 1 for the purpose of identifying electronically stored data as described in Attachment B.

**PROBABLE CAUSE**

14) On May 31, 2024, U.S. Customs and Border Protection (CBP) officers working at the DeConcini Port of Entry (POE) in Nogales, Arizona encountered a 2013 Nissan Pathfinder during primary inspection. The driver and registered owner was identified as Janet Felix-Madrigalos (FELIX). CBP officers also observed FELIX's juvenile daughter in the car. While at primary inspection, CBP officers noticed three mirrored glass columns in the cargo area of the vehicle. FELIX informed CBP officers that she was returning to Nogales, Arizona after picking up these mirrored glass columns that she bought in Mexico. A CBP officer lifted one of the columns and noticed that it felt heavy. CBP officers obtained a negative declaration from FELIX (including for narcotics) and referred her to secondary inspection.

15) Once at secondary inspection, a Z-portal scan of FELIX's vehicle revealed anomalies within the mirrored columns. CBP officers conducted a second scan of just the columns and confirmed that anomalies were present inside. A narcotics detection canine was then brought in and alerted to the odor of narcotics within the columns. During a subsequent search of the columns, CBP officers discovered one hundred (100) packages of methamphetamine with a total weight of 48.86 kilograms (107.70 pounds); three (3) packages of brown heroin with a total weight of 1.86 kilograms (4.10 pounds); three (3) packages of cocaine with a total weight of 2.06 kilograms (4.55 pounds), and eleven (11) packages of fentanyl pills with a total weight of 11.52 kilograms (25.04 pounds) concealed inside the mirrored columns. I know based on my training and experience, and after further investigation, that the value of the seized narcotics here can range from approximately \$2,500.00 to \$24,000.00 per kilogram depending on the narcotic.

16) FELIX was subsequently placed under arrest. Afterwards, law enforcement officers observed Target Device 1 receiving calls from a number with an area code out of Mexico. I know based on my training and experience that narcotics traffickers will often remain in contact with their co-conspirators and coordinators during the timeframe they are crossing the controlled substances to ensure successful entry, provide and receive updates, and

confirm successful delivery. Related to that, narcotics traffickers will also often not save contacts or save contacts with random letters or number to frustrate law enforcement's investigation to identify who they are communicating with.

17) HSI special agents conducted further investigation into FELIX and learned that she began crossing through the Nogales, Arizona POE using her 2013 Nissan Pathfinder on April 28, 2024. FELIX made two (2) crossings in April of 2024 (one through the pedestrian lane and one via the vehicle lane) and four (4) crossings using the vehicle in May of 2024, including the day of the instant offense. Notably, prior to these crossings, FELIX had not **crossed since March 31, 2014**, which is a ten-year gap. Moreover, all of 2024 crossings are followed by I-19 checkpoint northbound crossings. Based on my training and experience, I know that drug traffickers sometimes cross a vehicle several times, to include the checkpoint, to build up a crossing history as to minimize the risk of being referred at the POE when the vehicle is loaded with narcotics.

18) Based on the above, I believe there is probable cause to search Target Device 1 for evidence related to narcotics trafficking. This is based on the fact that Target Device 1 received a phone call from a number with a Mexico based area code during her arrest and after law enforcement found over one hundred (100) pounds of various narcotics inside FELIX's vehicle. As mentioned above, narcotic trafficking organizations will communicate via cellphones to receive updates on the delivery of contraband. Additionally, based on my training and experience, FELIX's crossing history suggests that she was building up a history so that she could avoid law enforcement's suspicion when crossing with narcotics. Lastly, given the amount of narcotics seized and their associated value, it is unlikely that a narcotic trafficking group would use a blind courier in this situation (*i.e.* someone who is unaware that they are transporting narcotics). In sum, a search of Target Device 1 could reveal information that would tend to identify those co-conspirators, reveal FELIX's role in the conspiracy, and potentially identify locations being used for drug smuggling (*e.g.*, the location of a stash house where FELIX was supposed to deliver the seized narcotics).

### **TECHNICAL TERMS**

19) Based on my training and experience, I use the following technical terms to convey the following meanings:

a) Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

b) Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c) Portable media player: A portable media player is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can

use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d) GPS: A GPS navigation device uses the Global Positioning System (GPS) to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e) PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f) Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g) Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h) IP Address: An Internet Protocol (IP) address is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer is assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i) Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

20) Based on my training, experience, and research, and from consulting the manufacturer’s advertisements and product technical specifications available online, I know that the target devices have capabilities that allows it to serve as a wireless telephone, receive and send email, instant messaging, a digital camera, and serve as a GPS navigation device.



## **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

21) Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on electronic devices. This information can sometimes be recovered with forensic tools.

22) Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the target devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that the following forensic electronic evidence might be found on the target devices:

a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b) Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c) A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d) The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how

a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e) Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23) Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of Target Devices 1 and 2 consistent with the warrant. The examination may require authorities to employ techniques, including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of the target devices to human inspection in order to determine whether it is evidence described by the warrant.

24) Manner of execution. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

///

//

/

/

**CONCLUSION**

25) I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the target device as described in Attachment A to seek the items described in Attachment B.

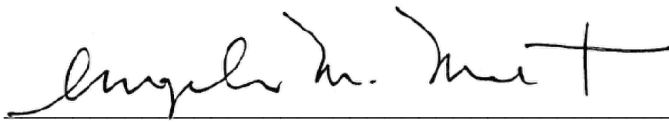
Respectfully submitted,

SELENA M DEACONS

Digitally signed by SELENA M  
DEACONS  
Date: 2024.06.11 16:40:46 -07'00'

Selena Deacons, Special Agent  
Homeland Security Investigations

Subscribed and sworn to before me telephonically,  
on June 12th, 2024.



The Honorable Angela M. Martinez  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**  
**ITEMS TO BE SEARCHED**

This warrant applies the following:

The property to be searched is documented on DHS forms 6051S as line item 0008, BLACK APPLE CELLPHONE, belonging to the event **2024260400049701**.

- a) Target Device 1 – Black iPhone with no case, a cracked camera, two cartoon stickers on the back of phone, and lock screen of a black and white rose picture.

Photos of Target Device 1 below:



**ATTACHMENT B**

The items to be seized from Target Device 1 to be searched are as follows:

1. All records on the device that relate to violations of 21 U.S.C. §§ 846, 841(a), and 952, conspiracy to possess and possession with intent to distribute controlled substances, and importation of controlled substances
  - a. Photographs or video depicting illicit narcotics, quantities of money, other co-conspirator(s);
  - b. SMS/MMS messages, voice messages, instant messages, third-party messaging application data, telephone numbers and notes, appointment books and/or calendars and notes, to-do lists, bookmarks, electronic mail, social media accounts, financial account information, contact lists, address lists, geo-location data, call logs, or any other data concealed within the electronic device to be searched that may relate to the suspected violations of federal law listed above;
  - c. Records recording the planning, commission, or concealment of the suspected violations of federal law listed above; and
  - d. Any and all micro-SD, memory cards or hard drives attached to or inside the electronic devices to be searched which are used as extended memory storage devices.
2. Evidence of user attribution showing who used or owned the device to be searched at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.
3. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer, smartphone or electronic storage (such as flash memory or other media that can store data) and in any photographic form.